Cyber Professionals in the Military and Industry—Partnering in Defense of the Nation

A Conversation between Maj Gen Suzanne Vautrinot, Commander, Twenty-Fourth Air Force, and Mr. Charles Beard, Chief Information Officer, Science Applications International Corporation

Transcribed and edited by Capt Jeffrey A. Martinez, USAF, and Capt Matthew R. Kayser, USAF

A strategic discussion on cyber is no longer an academic dialogue, and the associated technology is no longer the realm of industry or government development labs. The "defense" in the cyber domain is a national imperative; increasingly complex challenges force industrial and governmental seniors to expand collaborative efforts to address these challenges. Corporations across the globe are leveraging the cyber domain to deliver goods and services more quickly and cheaply while balancing the need to protect the personal information that customers entrust to them. Likewise, military commanders increasingly rely on integrated cyber capabilities to command and control and generate effects on the battlefield, both kinetic and nonkinetic. Safeguarding critical data, while allowing immediate access without interception or manipulation, is the key to mission success.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Professionals in the Military and Industry -Partnering in Defense of the Nation: A Conversation between Maj Gen Suzanne Vautrinot, Commander, Twenty-Fourth Air Force, and Mr. Charles Beard, Chief Information Officer, Science Applications International Corporation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute (AFRI),155 N. Twining Street,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**18**	

On 7 November 2012, two of our nation's senior cyber leaders, Maj Gen Suzanne Vautrinot, commander of Twenty-Fourth Air Force and Air Forces Cyber, and Mr. Charles Beard, chief information officer and senior vice president of Science Applications International Corporation (SAIC) sat down for a conversation. During this discussion, Mr. Beard recounted a journey of his efforts to reduce his company's cyber-attack surface and create a corporate environment resulting in a single enterprise information technology (IT) solution, and Major General Vautrinot not only articulated similarities in the Air Force's venture to defend the nation in cyberspace but also focused on how both the Air Force and industry can apply the lessons learned from successes like SAIC's migration as they continue to move toward a more homogeneous cybersecurity posture.

With their consent, we would like to share a private dialogue between recognized and mutually respected colleagues and partners in this dynamic domain. Additionally, interlaced into this conversation are contributions from each of Twenty-Fourth Air Force's operational cyberspace wings, which expound upon key discussion points and highlight current efforts to operationalize and normalize the cyberspace domain.

****

Vautrinot: Not surprisingly, your efforts resonate, and there is a true similarity of experience in this area. You've taken what were significantly diverse elements in a corporation and completely changed the dynamic—first organizationally and then technologically. I'm interested in which organizational changes you believe were most essential to that success; I'd like to leverage those changes toward our shared responsibility in this changing global environment.

Beard: Shared responsibility is correct. As we looked at cyber, we recognized that the governance model had to change. We grew up as 10,000 independent offices, and while that has its advantages from a market-development and a customer-responsiveness perspective, it

has its drawbacks from an enterprise IT governance and scale perspective. We needed strategic agility to engage in multiple global markets and in an increasingly hostile computer environment. The first step was to define and stabilize the environment, and that meant changing the way we thought about IT.

Vautrinot: In the military, major commands or functional organizations might be considered in the same way—all talented but very discrete . . . the description "cylinders of excellence" comes to mind. From a military operations stance, this makes sense, but it presents challenges when addressing threats and risk from a cyberspace perspective. Since information technology and communications grew up in a decentralized fashion, there's an apparent inertia toward retaining that decentralized approach. Yet, you've demonstrated the necessity in creating an enterprise solution to best operate what is now a cyber enterprise.

Beard: The first step for us was to make that connection and make sure we had a true enterprise view of the environment and begin to operate it as an enterprise asset—irrespective of how it originated. As the next action, we began to work with government to talk about the need to share threat information and improve our cyber posture. We [SAIC] operate IT environments on behalf of the government. We have client information on our networks, and we take the responsibility of stewardship very seriously. At the same time, however, we are a publicly traded company and operate on a global basis. We couldn't just take a US-centric view of how we were going to solve this problem anymore than the Air Force could take such a position. We had to change the intellectual reference for a lot of people when it came to governance and what it really meant as a multinational corporation to address this issue of cyber.

Vautrinot: In air and space domains, we had the advantage of developing unique and often superior or specialized systems: fifth-generation transitioning to sixth-generation aircraft and cutting-edge satellites . . . inherently unique. It was always about the military systems. Yet in cy-

berspace, it's a global, interconnected environment. We share the same man-made environment, and industry is at that "cutting edge." The military can't afford—technically or financially—to respond independently. We need shared responsibility—industry, government, academia, international partners—in altering the environment to our collective advantage and holding each other accountable for success. In military parlance, we can change the domain to provide freedom of movement to our allies while denying our adversaries the same. We're all working in the same space although perhaps we need to calculate risk and mission response a bit differently.

Beard: It's all about risk management and measured response. I go back to my Strategic Air Command days, where we operated in the nuclear domain. While the mission of deterrence was clear, the mission of strike was equally well understood. Preparing for both was the order of the day. Unlike the other domains within the military—ground, air, sea, and space—force projection and domination in the cyber domain are very difficult. You are running on shared infrastructure on a global basis, and the adversary often has an equal or better footing.

Vautrinot: I'm seeing a similar global dynamic in our support to remotely piloted aircraft missions. In order to provide mission assurance, we had to conduct extensive front-end research to understand the various links from the United States to the overseas flight. The system was designed with roughly 180 touch points, many of which are not military controlled, across several different networks, including foreign systems, making it critical to establish relationships with commercial organizations and allies. The security and assurance becomes a tremendous interdependency, which you are also seeing in industry.

Beard: In the commercial domain, interdependency equals continuity of operations and risk management. There is a difference in the way we view the threat, but mission assurance for a commercial company is largely driven by the markets and geographies in which it operates and the type of operation it is conducting. The fact that those operations are

conducted on globally shared infrastructure is an important context for corporate executives to understand as they consider risks.

Vautrinot: The commanders we support have indicated a similar imperative for uninterrupted access to trusted and verifiable data. Mission assurance in the cyber domain is so foundational to the mission that we can't afford to lose the capacity to communicate—it's essential to military command and control.

Beard: That's exactly right. A company can have the greatest capabilities in the world, but if it cannot operate in the digital domain and if it cannot sustain uninterrupted access to the energy and communications infrastructure, it's very difficult to have a mission profile that survives. So we see command and control very much alike in the context of the military and commercial mission because we're trying to conduct business operations around the globe. If I cannot provide access to clean communications and uninterrupted energy, then the business continuity is dramatically impaired.

Vautrinot: At a corporate level, you had to go beyond awareness. People had to get on board, understand the codependency, and see its benefit to the individual. Having the discussion on a smaller scale makes the effect tangible and makes change acceptable. A successful business can leverage this to shift a company in new directions. Was the realization something that was tailored to each individual and scaled, or did senior leadership have to drive enterprise awareness to change organizational culture?

Beard: At SAIC, we are fortunate to have people on our board who have walked the halls of government and industry, who understand that this threat is real. So what we began to do was translate that risk in the context of the business. I think what you'll find is that various commercial industries are further along in that understanding, that maturity. Certainly the financial services industry has understood it for many years. They have separate risk committees on their boards of directors, and it's one of many risks that they must consider. You've got other industries, like energy, where the awareness is ratcheting up

even further. They witness the threat vector changing from simple intelligence gathering to operational destruction, as indicated by the Saudi Aramco case.[1] In the health-care industry, a company might spend a decade and $10 billion building out a product or a new drug, only to see a carbon copy of that product launched in a foreign country a year before they get approval from the Food and Drug Administration [FDA]. All their intellectual property is gone, so the revenue stream anticipated by that company for that product for the next 10 years is significantly cut. The economic imperatives are becoming the clear and present danger to the national economy where these businesses operate, but many companies still don't understand cyber threats and their possible impacts, both physical and economic.

Vautrinot: There is similar recognition concerning cyber dependency. However, I'm not sure there's cognizance on the level of dependency, and our ability to conduct all missions—to fly, fight, and win in air, space, and cyberspace. Our challenge as we move forward is to create linkage in all mission elements . . . the operational tapestry versus the mission threads. As we expand on this focus, we must be cognizant to balance these operational efforts with the ability to maintain and defend our networks. Under the Twenty-Fourth Air Force, the 689th Combat Communications Wing specializes in maintaining this equilibrium by extending cyber capabilities to the tactical edge in support of the war fighter while continuing to provide defensible, trusted communications at that edge.[2]

Beard: The fact that e-mail is routed to servers beyond your company networks and possibly national borders—perhaps to countries that have lawful intercept laws that are different than your own—is simply not understood by the casual user. We've built entire businesses that depend on the cyber domain, but we don't really understand the security challenges associated with that domain. It is daunting when you begin to understand what the impacts really could be, and that is why leadership is so critical to navigating this challenge, and the endless extension of network reliance.

Vautrinot: In the current budget environment, there's a complicating factor: the expected resource commitment actually closes the dialogue and decision space before options can be explored. The complexity of this enterprise-level transformation becomes its own kind of inertia. If cyber is currently disordered, then we're caught somewhere between the natural "entropy" of the domain and the inertia of the decision. Did you fight that on the industry side?

Beard: I recently heard an attorney suggest that corporate directors should not be better informed on cybersecurity risks because the laws protect them on things for which they are not educated. I found that to be a shortsighted view. I think in the context of commercial industry—take a bank, for example, a public utility, a pharmaceutical life sciences company, or a defense contractor—the foundation of these businesses is reputation and trust. The boards of those companies, with robust risk-management practices, know best if they're in an informed position to adjudicate those risks. To us, the cyber risk may be the most dominant risk that we think they face. But for a defense contractor, perhaps the biggest risk they're facing is that they have people in harm's way. A financial institution may be facing a liquidity crisis. A pharmaceutical company may be concerned about achieving FDA approval to meet forecasted sales and finding the counterfeit versions of their products selling around the globe. The question is how well articulated is that risk, and this notion that we can just build a fortress around the business with static cyber defenses is simply the digital version of the Maginot Line.

Vautrinot: Agree, static defenses didn't work in World War II and won't work in the cyber environment. That's why in the Air Force, we've been focusing on a proactive defensive posture. Instead of waiting until an adversary penetrates our networks to assess our vulnerabilities, we have created specialized teams that search our networks and seek out those vulnerabilities, preferably before they are exploited. We focus on identifying and defending those interfaces that are essential to mission success—Gen Keith Alexander, commander of

US Cyber Command, would call this capability "recon/counter-recon." A key facet of this defensive effort is identifying and focusing on a commander's prioritized "defended asset list," those critical areas that must be able to operate through a contested environment or attack. This corresponds directly to something we spoke about before: linking our efforts to the operational mission. We can enter a network environment and provide the commander who is reliant on that system with timely, accurate decision information. Specifically, can he rely on the network system to successfully accomplish the mission?

This proactive posture is bolstered by the information and threat vector sharing between industry and government. A superb example was the Department of Defense's Voluntary Defense Industrial Base Cyber Security / Information Assurance Program, an agreement in which companies, including many of the larger corporations in this country, collaborated with the Department of Defense (in the Air Force, via the Air Force Computer Emergency Response Team under the 67th Network Warfare Wing) and Department of Homeland Security to share sensitive threat information and thereby improve the collective cyberspace defense.[3]

Beard: What you are beginning to see now on the commercial side is a frustration with being on static defense. The underlying economics of cyber attacks currently favor the adversary just as improvised explosive devices favor insurgents. To counter that model, we have partnered both with industry and government to develop trusted platforms that allow for dynamic defenses through our Cloudshield products. Alternatively, some in the commercial markets believe it is time to punch back. This move from the cyber operations perspective is to move from computer network defense to computer network attack. I have real concerns about commercial companies taking on a computer network attack type of mission, with unintended consequences both for law enforcement and other government agencies.

Vautrinot: Historically under international law, the concept of attack was the province of the nation-state. However, geographic boundaries

no longer demarcate actors on the offensive; for example, we've seen companies selling services purporting to respond to cyber intrusions by sending reset commands or redirecting malicious traffic. The nature of cyber is that companies may well have the capability to go much further. In doing so, they will contend with domestic law as well as statutes where they are operating or causing effects. Unfortunately, current domestic and international policies haven't kept pace with the advancement in cyber capabilities; therefore, loopholes and outright gaps in governance exist that can be leveraged by bold corporations.

In the Air Force, we aren't just constrained by domestic laws but also by government policy. Generally, the Department of Homeland Security is responsible for defending cyber assets outside the Department of Defense's networks, but regardless of which organization is contemplating these actions, the problems of definitively attributing an intrusion to a particular attacker and deconflicting actions with other entities are particularly difficult. This again highlights the need for an information-sharing framework between government and industry that facilitates rapid action to cyber events.

Air Force senior leaders are certainly aware of the vulnerabilities of our network systems, but now there is also a keen recognition of the opportunities to enable defense as well as facilitate mission success. A great example has been our work with US Transportation Command and Air Mobility Command. Their dependencies are not limited to the .mil domain but on the .com and the ability to work with industry partners to ensure worldwide movement. As a result, they are acutely aware, and the understanding causes them to be very proactive in terms of resolution. Yet in other commands, there is resistance and belief that their networks are "private" or separate from the global Internet and therefore its inherent adversaries. In regards to your independent offices, did you experience similar variance?

Beard: We did. We had employees, partners, and even clients who operated on what they believed to be "closed" networks; therefore, they didn't feel like they had a problem. They simply did not see the

need for added layers of protection or policy enforcement on their activities. What they called bureaucracy is what we call mission assurance in the context of systems engineering.

Vautrinot: Clearly, a necessity for unity of effort and with it a clear chain of responsibility—command and control. Certainly, you were implementing an enterprise solution for all the right reasons, and the field of independent offices realized the importance. Nevertheless, there is resistance to losing what some believe is their self-actualization—their ability to control. What allowed you to bridge that natural resistance in the field and drive the implementation?

Beard: I would say three things. One was the commitment of leadership. You had to have the will of the leadership to say, "We're willing to go here." Second, we began to educate the leadership, management, and select employee groups. That was really important to us—to increase the awareness. Finally, we had to rethink the context of cybersecurity. We needed to understand what truly had to be protected and where we would establish trust. The results of that exercise materially changed our defense-in-depth strategy.

Vautrinot: What level of leadership was necessary to initiate? In our vernacular, it would be the major commands and key functionals saying, "OK, we're all in agreement. We recognize the threat, and we're all going to move together in this direction." Then it would be our responsibility to help them understand the rationale for implementing measures or taking action that may be locally restrictive.

Beard: Correct, not everybody agreed. It took a combined chief executive officer / chief operating officer / chief financial officer–level mandate, and we broke some china.[4] Although people understood the leadership decision and the need for policy enforcement and oversight, they still wanted autonomy, so we then developed tools to provide autonomy while preserving the security posture. That was done in the context of productivity and giving people what they wanted. What we didn't understand 20 years ago, when operations in the digital domain began to evolve, was this cyber-risk issue. The risk issue has

now raised its ugly head, and you can't ignore it, so you're conflicted. I want to take care of you as an end user, as a customer, but I have this other responsibility that you may or may not understand or appreciate, and I'll try to help explain it. I just can't explain it to every end user because I don't have the cycles to do that because then I'm not doing my job. So that's part of the balance.

Vautrinot: You are protecting the long-term viability of the corporate entity, the same way that we're protecting the long-term viability of the mission and our support to the nation. There has to be some freedom of action, across the enterprise, to allow that protection.

I believe that in industry you also have a requirement to report, not cybersecurity per se, but your viability as a corporate entity in the realm of cybersecurity. If I had a similar report, I anticipate we wouldn't receive a passing grade. However, we have moved toward a construct where there's both asset- and enterprise-level management, but only on the .mil and the .smil networks. Each of the mission system networks defines itself separately and is independently resourced and managed. In your model, there'd be one "general" who would be designated to control asset management of all Air Force network interfaces, soup to nuts—precisely what you had to do in industry. Certainly necessary, but I've learned that operational viability in this contested environment requires a fundamental change to the assets we would centrally manage—it requires sensoring to enable awareness and proactive response to threats within the network. The first step, having the asset management, by itself is insufficient, but being able to sensor it—to get that situational awareness and to allow your system to react in an automated fashion—is the next step. How did you approach the engineering-level changes?

Beard: That was part of the second journey in this process—to instrument and do all the enterprise vulnerability analysis and the scans against that baseline. This allows you to prepare for continuous monitoring. The reason that it's important is what makes up the third journey: I may want to morph my network based on the business mission,

actionable threat intelligence, and the intent of select adversaries that are active.

Vautrinot: This is where cyberspace operations can facilitate mission operations or provide mission alternatives. We don't need to command and control the mission, but we need to have full visibility of what's going on in the [cyber]space and be able to adjust it in real time to thwart adversary positioning. It makes the adversary's problem set much more difficult while preserving mission effectiveness.

Beard: Exactly. Because if adversaries understand your network better than you do, you've got problems, and if your computer infrastructure is so rigid that you can't dynamically allocate, they're going to take advantage of that, and once again both the economic and operational advantages go to the adversary. This is why we moved to the hybrid cloud model—because it gave us the opportunity at the application and data level to move workloads around. I can now take a workload that has historically operated on specific servers in a specific data center and dynamically assign that workload to virtual machines operating in virtual data centers that may have very different geographic characteristics. Information can stay within my data center, but I can move it to different places.

Vautrinot: In that construct, for example, employee health care doesn't own medical data, and the finance department wouldn't own financial data. Moving and providing access to desired data within the enterprise is the key, and each branch of the enterprise is using that data rather than controlling it as a segregated element. The goal shouldn't be to control but rather have trusted data accessible anytime, anywhere. Our challenge is breeding an environment that is constantly agile.

There appears to be a bit of a misnomer surrounding IT efficiency "savings." Talking to AT&T, Microsoft, and industry partners like you, the front-end investment to make that change is not only an investment of corporate culture and leadership but also a significant capital investment. Not just to save money over the long-term operation of

the IT but a financial investment in cybersecurity. How did your corporation work through the investment dynamic to determine that the company had an imperative to afford cybersecurity? What was the scope of that assessment and dialogue?

Beard: We didn't try to make it about saving money on the front end. We tried to make it about strategic agility and what that meant to us as a global corporation. We knew that we needed agility at the enterprise level. So by making this investment, it began to give us the ability to start flexing. Think of it as not just using this technology to operate companies but in the context of how to virtualize companies and recombine them. Indeed, SAIC is going through such an activity at this time, and it is exciting to see IT as an enabler rather than a roadblock.

Vautrinot: Cyber in this context that we are describing—it is a mission, and you're not viable without this mission. Despite our current national economic situation, we have to transition dialogue from cost reduction to the defense imperative and therefore worthy of the investment from a national strategy standpoint.

Beard: We pulled cyber out separately from a budget perspective and treated it as a strategic investment. If you look at IT as a cost center, you will miss the opportunity. I've advised a number of companies over the years that looked to IT cost-reduction targets as a way of meeting a corporate cost objective, but the dirty little secret is that they take on technical debt that shows up neither on the balance sheet as an unfunded liability nor on the enterprise risk register.

Vautrinot: In that vein, my "technical debt" is lack of automation and sensoring, which I'm overcoming manually—in effect a huge workforce that isn't sustainable or appropriate in a dynamic cyber environment. It drives reactionary responses to problems and precludes resourcing automated sensoring and solutions.

Our efforts to move from a dispersed, installation-managed network to a single, homogeneous, and centrally managed network will allow the follow-on of necessary sensoring and automation to free up

resources and robust network operations at the scale required for a global industry, like yours, or military operations. Until then, this drives a large back-end cost.

Beard: We all know that reactive posture is more expensive. We would never do that with a weapons system development effort—we try to design solid engineering into the front end. It's a lot cheaper in the long run to do it in that order.

Vautrinot: The assumption is that the things you see, you can at least deal with, but what about the unknown unknowns?

Beard: The unknown unknowns are unacceptable. For Sarbanes-Oxley Act purposes, for example, we are required to have preventive controls in place.[5] The unknown unknowns force you to think "left of bang."[6] But that then leads you to the realization that you can't protect everything. So let's have a business dialogue or a military dialogue about the assets—could be data assets—that we wish to protect.

Vautrinot: It's what I referred to as the defended asset list but at a discrete level instead of an enterprise level. We've worked individually with the Tanker Airlift Control Center as well as one of the many air operations centers to demonstrate this dynamic. But we cannot apply it at an enterprise level because we can't "see" or control the cyber assets in the enterprise.

Beard: In my role, I'll get a phone call that says, "I have this urgent information security problem; come help me." And the first two questions are, "When were you made aware of a requirement to protect this asset?" and "When did you know you had this problem?" If it wasn't on the defended asset list, I didn't proactively do anything to protect it, and if it's been exfiltrated or manipulated, I didn't specifically look to ensure it didn't go outbound or preserve its baseline. So if the defended asset list is incomplete, it's very difficult for me to develop and implement a cybersecurity policy to protect and defend those assets. This is a team sport, and there is shared responsibility in mission assurance that is incredibly dynamic. If you simply buy a security appliance, by

the time you deploy it, it's out of date. So you have an asymmetric threat, and you are trying to respond to it with a traditional legacy process. It's counterproductive, which is why we are looking to change the game.

Vautrinot: Absolutely, that's why we are building a platform that can be constantly adjusted. If I used a space operations comparison, I define the interface of the payload with the platform. That means I need to own the platform and the enterprise and can adjust in real time. For example, under Col Paul Welch, commander of the 688th Information Operations Wing, we developed the Information Operations Platform to provide an accredited open-architecture framework for rapid deployment of other third-party applications.[7] This ability to swap our tools allows accelerated fielding and deployment of those tools, providing dynamic and responsive operations for Air Force and Department of Defense cyberspace operations. This provides flexibility—like a fighter aircraft, which can be configured for an air-to-ground mission during one sortie and for an air-to-air mission during the next. The difference is that the fighter is reconfigured in hours/days, whereas in cyber it's got to be seconds.

Beard: Let's say my intrusion detection system has been defeated and I need something new. The software base is part of a platform and it's nonnegotiable, so the hardware platform itself doesn't change. I can deploy it right now. It's this stealth machine with out-of-band controls that only we see, but I can put different payloads on it.[8] The independent offices can do what they need to do, but the enterprise can still dominate the network on their behalf. That's the trick—command and control at the enterprise level with decentralized execution, a dynamic environment that provides enterprise agility and "trust" built into the platform that is highly configurable and allows you to look "left of bang."

Vautrinot: The intent as we continue to refine our skills in this domain is to move from the reactive to the proactive posture and present agile, sensored targets to our adversaries. All of us, whether govern-

ment or industry, are in the business of trust: we must use the available intellectual capital and emerging technologies to protect our information and systems from being linked into an expansive, malicious chain [2011 global remediation cost $388 billion].[9] The nation's cyber journey is a shared responsibility, and it's personal—only through developing partnerships can we continue to defend this nation in cyberspace.

****

The sheer scope of this domain is difficult to grasp: in the next 60 seconds, 168,000,000 e-mails will be sent; 695,000 status updates will be posted to Facebook; and 690,000 searches will be conducted on Google.[10] As the opportunities afforded by this domain continue to multiply, so do the vulnerabilities. Those of us who were present for this discussion left the room not only with a greater understanding of the challenges that lie ahead in this domain but also with a greater appreciation for the collaborative efforts occurring between government and industry to safeguard the critical information that corporations, commanders, and the country rely upon. ✪

Notes

1. In one of the most destructive acts of computer sabotage as of this writing, on 15 August 2012, a virus erased data on three-quarters of Saudi Aramco's corporate computers, posting a burning US flag in place of that information. Because of the attack, the company was forced to replace tens of thousands of hard drives.

2. The mission of the 689th Combat Communications Wing is to train, deploy, and deliver expeditionary and specialized communications, air traffic control, and landing systems for humanitarian-relief operations and dominant combat operations—anytime, anywhere. To keep up with the rapidly changing strategic environment, combat communicators rely heavily on industry to provide commercial off-the-shelf technology, which enables them to extend, operate, and defend cyberspace capabilities in the most austere locations, in the most effective manner possible.

3. Ensuring the defense of military information and systems—both through computer network defense and computer network attack—is a daily challenge. The 67th Network Warfare Wing executes Air Force network operations, defense, attack, and exploitation to create integrated cyberspace effects on behalf of Twenty-Fourth Air Force and the combatant commands. The wing operates within current Department of Defense authorities to protect Air

Force and Department of Defense information and systems and to ensure freedom of maneuver in the cyber domain. The 67th includes the on-net operators responsible for the day-to-day operation of Air Force networks. Extensive collaboration between the wing's personnel and other government and civilian organizations ensures the continuous sharing of cyber threat information across public and private entities.

4. Just as "a bull in a china shop" breaks china. In this case, the introduction of cybersecurity processes broke normal business processes.

5. A congressional bill enacted in 2002, the Sarbanes-Oxley Act is also known in the Senate as the Public Company Accounting Reform and Investor Protection Act, and in the House of Representatives as the Corporate and Auditing Accountability and Responsibility Act. The bill was enacted due to a number of major corporate and accounting scandals, including those involving Enron and WorldCom.

6. The term *left of bang* refers to a timeline in which each marked incident is a "bang." Activities "right of bang" are reactive responses to the incident; those "left of bang" are proactive actions in preparation for such incidents.

7. The 688th Information Operations Wing delivers these proven information operations and engineering infrastructure capabilities integrated across the air, space, and cyberspace domains. The wing has developed an innovative, rapid tool-development process accompanied by a rapid-acquisition program that reflects immediate, medium, and long-term systems approaches. The innovation framework involves Air Force Materiel Command (AFMC) working with Air Force Space Command to establish a center of cyber innovation to provide cost-effective cyberspace capabilities, such as the Information Operations Platform, in the appropriate time frame to support the joint war fighter.

The 688th expands the innovations achieved by the research topic of interest, hosted by Colonel Welch, by locally partnering with science and technology expertise from the Air Force Research Laboratory and simultaneously joining with their acquisition counterparts such as Col Chris Kinne, from AFMC in San Antonio, to expand local acquisition authority delegated from the Office of the Secretary of the Air Force for Acquisition. A diverse, colocated knowledge set is required to complement the resident cyber-development expertise. Lt Col Jim Smith leads the Air Force Operational Test and Evaluation Center's presence in this new organization to test and verify the effectiveness of proposed capabilities in an operational environment.

8. Out-of-band control passes control data on a separate connection from main data.

9. *Norton Cybercrime Report 2011*, Symantec Corporation, 7 September 2011, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/.

10. "60 Seconds—Things That Happen On Internet Every Sixty Seconds," GO-Gulf.com, 1 June 2011, http://www.go-gulf.com/blog/60-seconds/.

Maj Gen Suzanne M. Vautrinot, USAF

Major General Vautrinot (USAFA; MS, University of Southern California) is the commander of Twenty-Fourth Air Force, Air Forces Cyber, and Air Force Network Operations, Lackland AFB, Texas. She is responsible for the Air Force's component numbered air force providing combatant commanders with trained and ready cyber forces that plan and conduct cyberspace operations. The general directs the activities of three operational cyber wings—two headquartered at Lackland and one at Robins AFB, Georgia—as well as the 624th Operations Center at Lackland. General Vautrinot has served in various assignments, including cyber operations, plans and policy, strategic security, space operations, and staff work. She has commanded at the squadron, group, and wing levels, as well as the Air Force Recruiting Service. The general has served on the Joint Staff, the staffs at major command headquarters, and Air Force headquarters. Prior to assuming her current position, she was the director of plans and policy, US Cyber Command, Fort George G. Meade, Maryland, and the special assistant to the vice-chief of staff of the US Air Force, Washington, DC. A National Security Fellow at the John F. Kennedy School of Government, Harvard University, General Vautrinot is a distinguished graduate of Squadron Officer School, Air Command and Staff College (with honors), Joint and Combined Staff Officer School, and Air War College (correspondence).

Charles E. Beard Jr.

Mr. Beard (BS, Texas A&M University; MBA, University of Montana) is the senior vice president and chief information officer for Science Applications International Corporation (SAIC) and general manager of the SAIC Cybersecurity Business Unit. In this dual role, he has led SAIC to become the first in its industry to transition the enterprise to a cloud computing infrastructure and address the security and control challenges inherent in that journey. He is secretary of the Inova Health Care Services Board of Trustees and chairman of the Quality Board at Inova Mount Vernon Hospital. Prior to joining SAIC, Mr. Beard was a director in the Oliver Wyman division of Marsh & McLennan. In this role, he provided strategic advisory services associated with corporate transactions and restructurings and developing information technology strategies to achieve business design objectives. He also served as the senior vice president for Global Transportation and Industrial Markets at KPMG Consulting (later BearingPoint), leading the company's strategy and operations services for global commercial clients, including GE, Honeywell, United Technologies, and Southwest Airlines. He has completed continuing education at the Harvard Business School and MIT Sloan. Mr. Beard is a featured speaker at the university level and a frequent contributor to major media publications.

Let us know what you think! Leave a comment!